

IaC Template Suite for Credential-Free Workload Identity Provisioning

By: Albin Rönkvist & Piran Amedi

Overview

- Introduction
- Methodology
- Implementation
- Results
- Analysis and Discussion

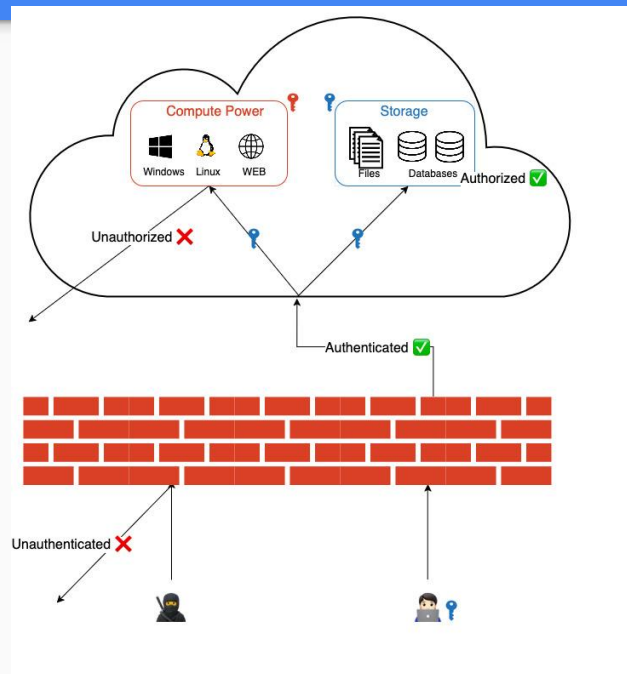
Introduction

Background

Introduction - Background

Cloud computing & Identity and Access Management (IAM)

- Cloud providers deliver computing services over the internet
- IAM manages access via:
 - **Identities (who)**
 - **Roles (what)**
- Workload Identities (e.g., applications, services, scripts)
 - **Internal:** within cloud provider
 - **External:** outside of cloud provider



Introduction - Background



IAM

- **Provisioning IAM:** How is IAM infrastructure provisioned?
- **Workload authentication:** How does a workload identity authenticate?

Introduction - Background

Provisioning IAM



Purple: getting started
Blue: scaling

Alternative	1: Manual Configurations 	2: Infrastructure as Code (IaC) 
Method	Cloud provider portals or ad-hoc scripts	Everything as code
Adoption	✓ Simple to get started with built-in automation	⚠ Initial development effort
Feature Support	✓ Supports all native cloud provider features	⚠ IaC tools may lack full feature support
Security	⚠ Limited testability, visibility and collaboration	✓ Visibility, tests, peer reviews.
Consistency	⚠ Prone to configuration drift, lacks reproducibility	✓ Single source of truth, preventing drift, reproducibility.
Maintainability	⚠ Operational complexity at scale	✓ Version control, reusable components.

Introduction - Background

Workload Authentication

Purple: getting started
Blue: scaling

Alternative	1: Long-lived static credentials 	2: Credential-Free 
Method	Secrets, certificates, passwords, access tokens.	<ul style="list-style-type: none">• Internal workloads: Cloud-managed Identities (e.g., Azure Managed Identity)• External workloads: Federated authentication, IdP (e.g., GitLab)
Adoption	✓ Simple to create	⚠ IdP-specific configuration, more identities
Feature Support	✓ Supported in most workloads	⚠ Less support among workloads
Security	⚠ High exposure risk and too flexible	✓ Eliminates the risk of secret exposure, fine-grained control
Maintainability	⚠ Requires secure storage and frequent rotation	✓ No need for storage or credential rotation






Introduction

Problem Statement

Introduction - Background

Problem Statement

Purple: getting started
Blue: scaling

Alternative	Alternative 1  	Alternative 2   
Method	Manual configurations & Long-lived static credentials	IaC & Credential-Free
Adoption	✓	⚠
Feature Support	✓	⚠
Security	⚠	✓
Consistency	⚠	✓
Maintainability	⚠	✓

Introduction

Motivation

Introduction - Motivation

- Need for workload IAM infrastructure
 - With ease of adoption
 - With feature support
 - With security, consistency, and maintainability

Introduction

Aim

Introduction - Aim

- A template suite for Workload IAM infrastructure
 - **IaC**-driven for security, consistency and maintainability
 - **Credential-free** authentication for further security and maintainability
 - Ease of adoption with installable **templates**
 - Feature support with **workarounds**

Introduction

Scope

Introduction - Scope

- **Includes:**

- **Solution:** IAM infrastructure provisioning
- **Cloud & Identity providers:** Azure, Microsoft Entra ID, & GitLab
- **IaC & DevOps providers:** Pulumi, GitLab, & Docker
- **Programming languages & platforms:** C# & .NET

- **Excludes:**

- Other cloud providers & programming languages
- Security auditing & risk detection

Methodology

Methodology

Requirements

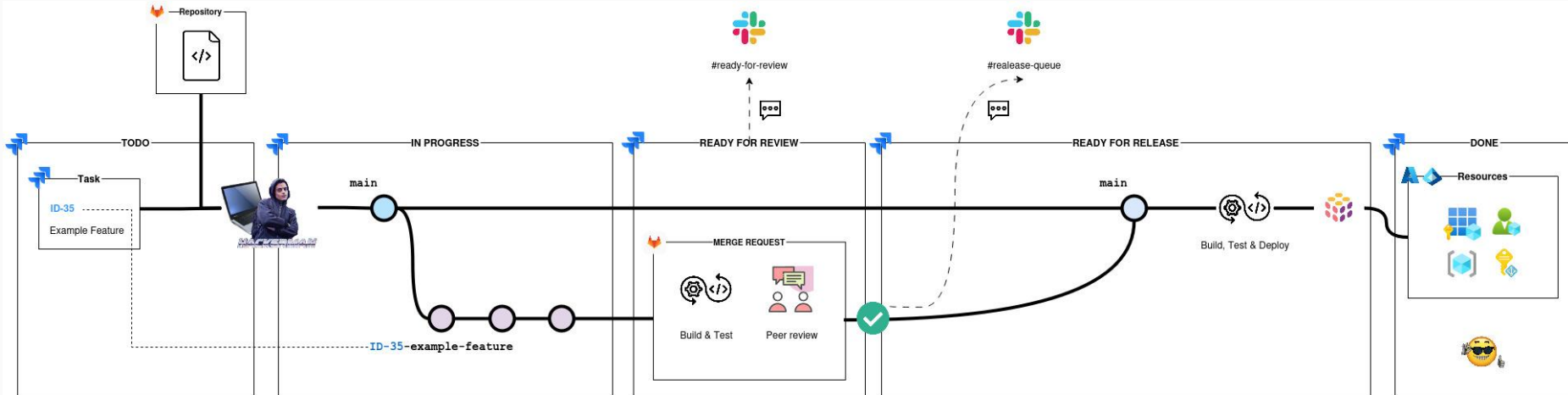
Functional Requirements	
ID	TITLE
FR1	Install Template Suite
FR2	Generate Projects from Templates with Custom Parameters
<u>FR3</u>	Publish NuGet Packages for Common Components
FR4	Setup IAM-provisioning IaC Projects
<u>FR5</u>	Include CI/CD pipelines in projects
FR6	Manage IAM-provisioning IaC Projects
FR7	Provision Microservice Resources
FR8	Access Microservice Resources

Non-Functional Requirements	
ID	TITLE
QR1	Optimized System Performance
QR2	Code Readability
QR3	Reusable Components & Modularization
QR4	Testability
QR5	Documentation
QR6	Credential-free Workload Identities
QR7	IAM Role Least Privilege Enforcement

Methodology

Development Method and Workflow

- Kanban
- CI/CD
- Trunk-based development

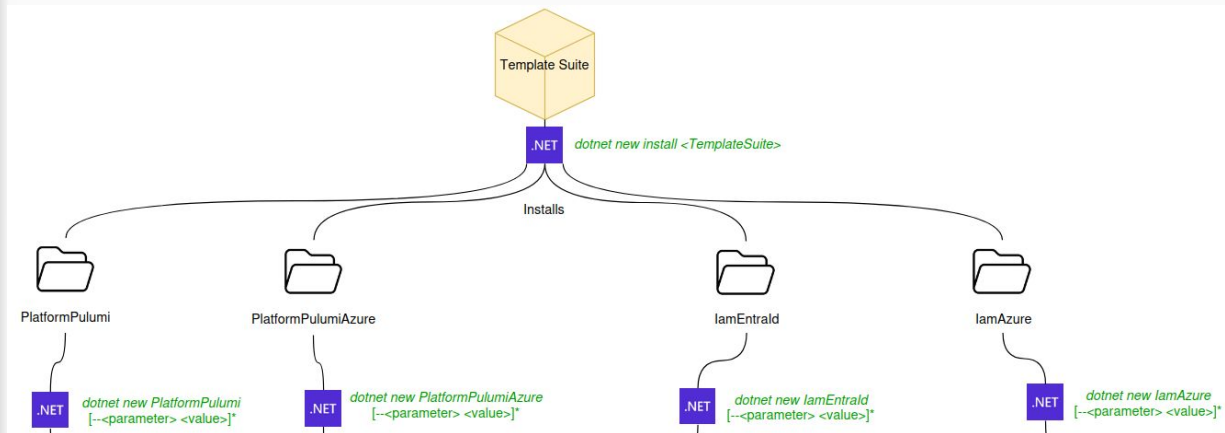


Implementation

Implementation

Template suite (FR1, FR2)

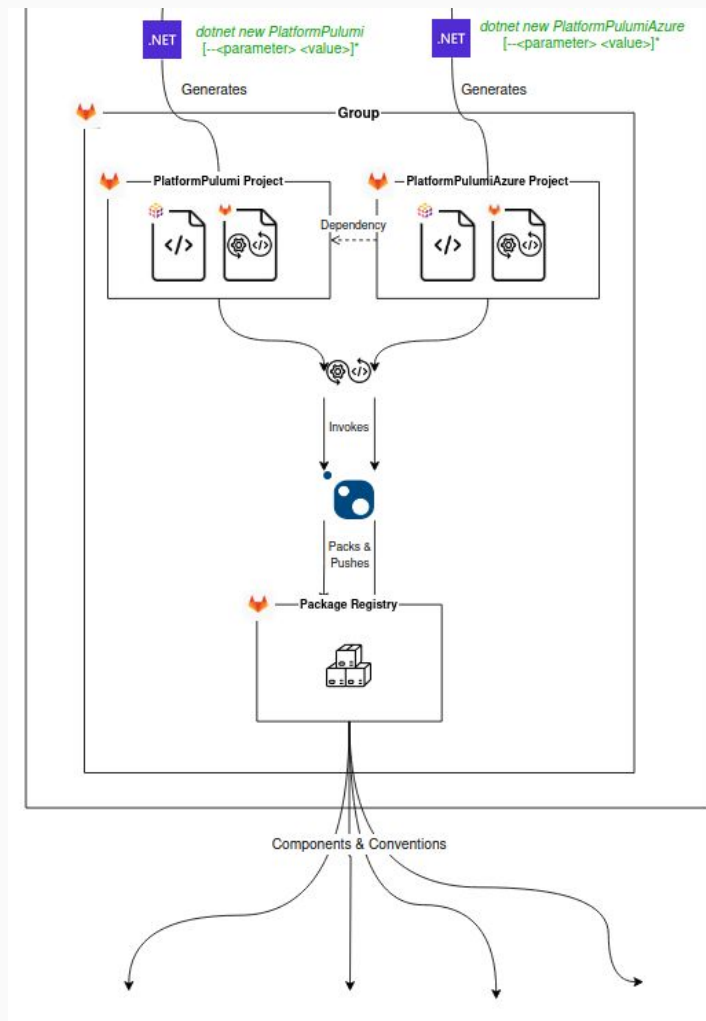
- Container for templates
 - .NET template engine
-
- Installable template suite (FR1)
 - Generates projects with custom parameters (FR2)



Implementation

Platform projects (FR3, FR5)

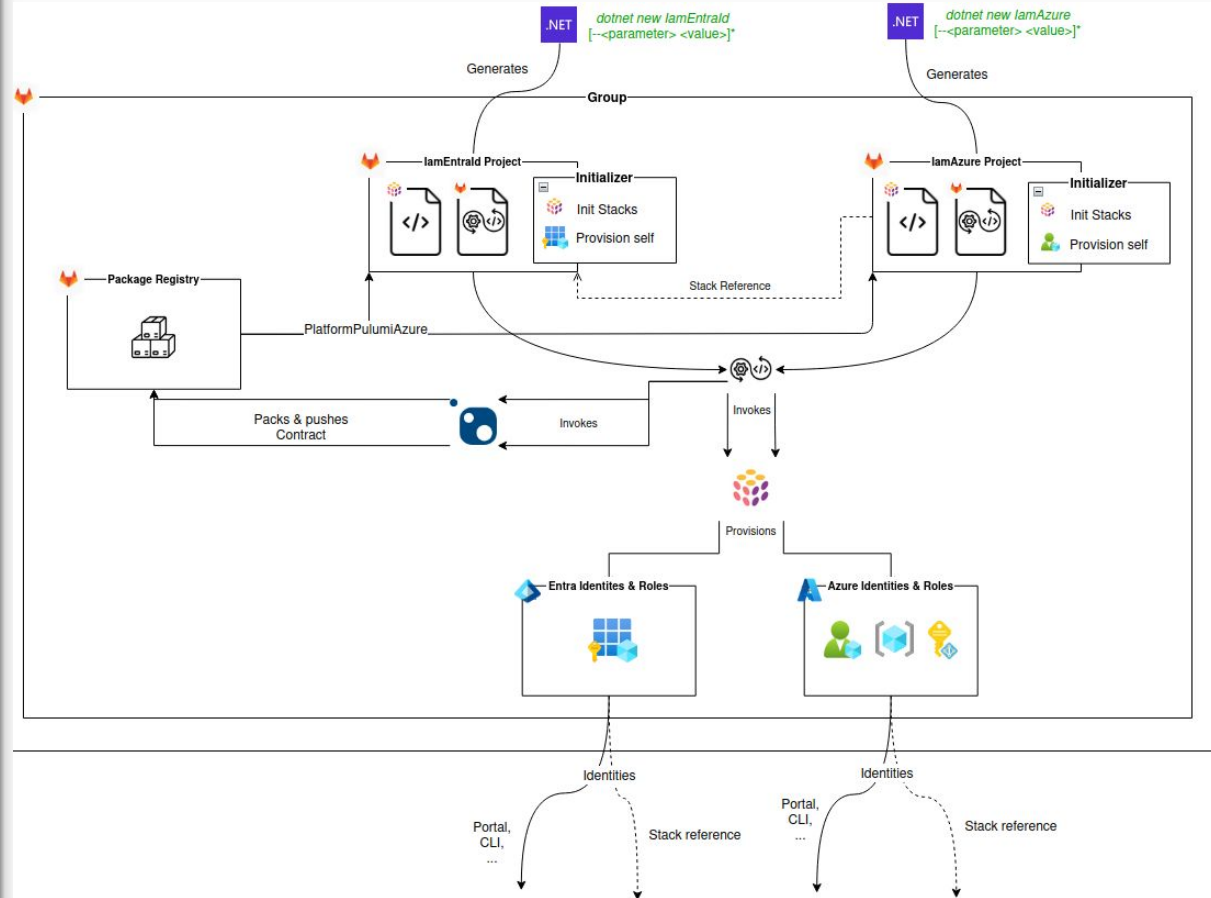
- PlatformPulumi
- PlatformPulumiAzure
- Common components NuGets (FR3)
- CI/CD pipeline (FR5)



Implementation

IAM projects (FR4-6)

- lamEntrald Project
- lamAzure Project
- Initialize IAM (FR4)
- Manage IAM (FR6)
- CI/CD pipeline (FR5)



Implementation

IAM projects - lamEntrald

- Initializer Project

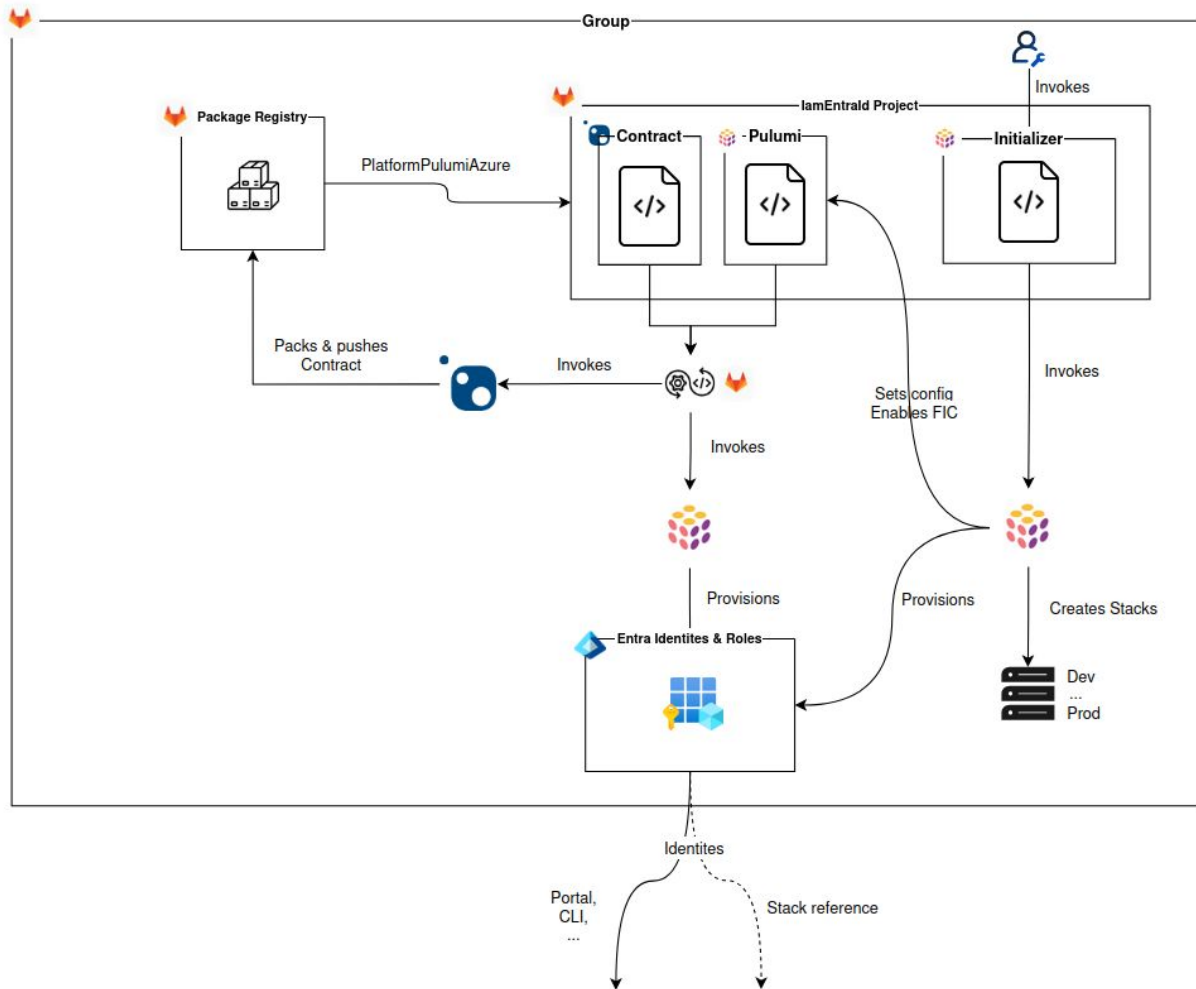
- Creates stacks
- Runs the *Pulumi Project* (self-assign)
- Sets configuration (enable FIC)

- Pulumi Project

- Applications
- Service Principals
- Directory Roles
- API permissions
- Federated Identity Credentials (FICs)
- Stack references

- Contract Project

- Contracts for stack references



Implementation

IAM projects - lamAzure

- **Initializer Project**

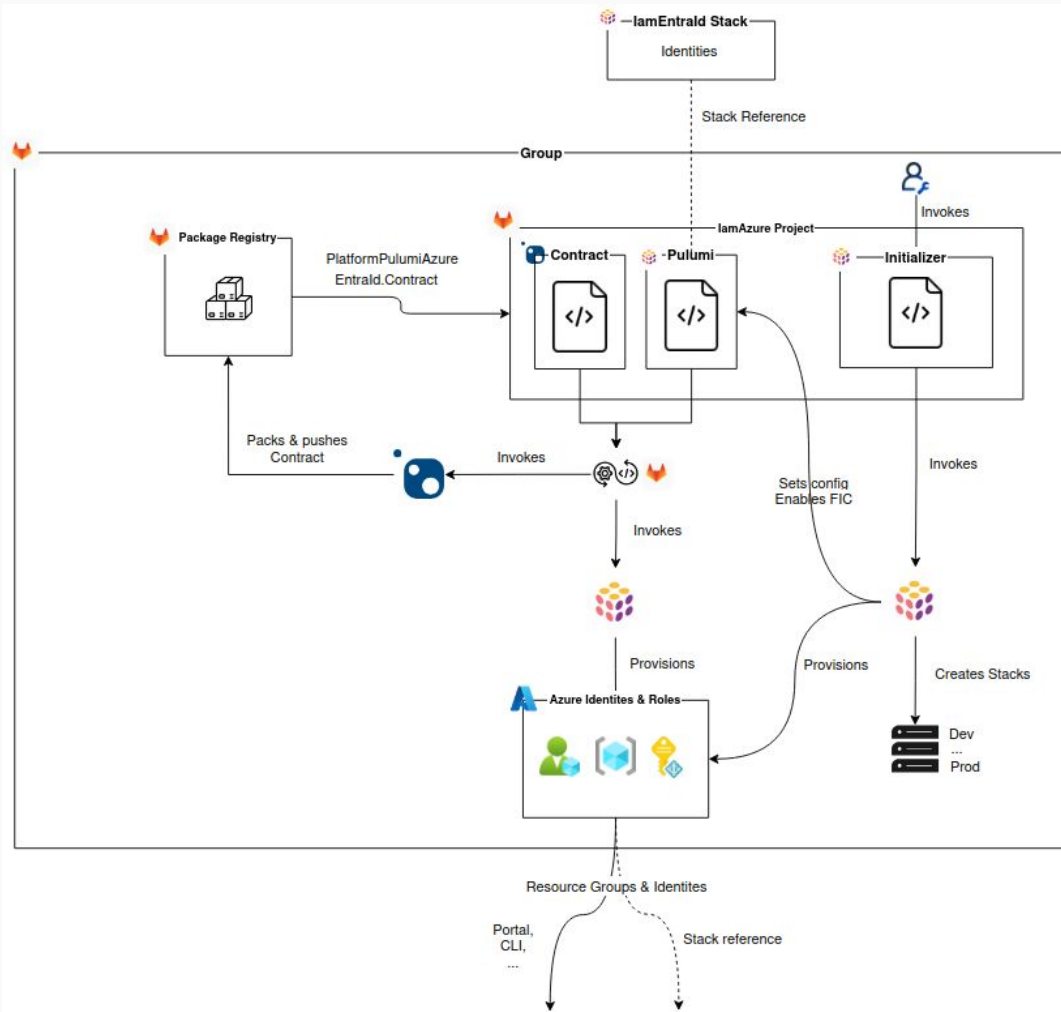
- Creates stacks
- Runs the *Pulumi Project* (self-assign)
- Sets configuration (enable FIC)

- **Pulumi Project**

- Resource Providers
- Resource Groups
- Managed Identities
- Azure roles (RBAC)
- Stack references

- **Contract Project**

- Contracts for stack references



Implementation

Least privilege access

- **lamEntrald workload:**

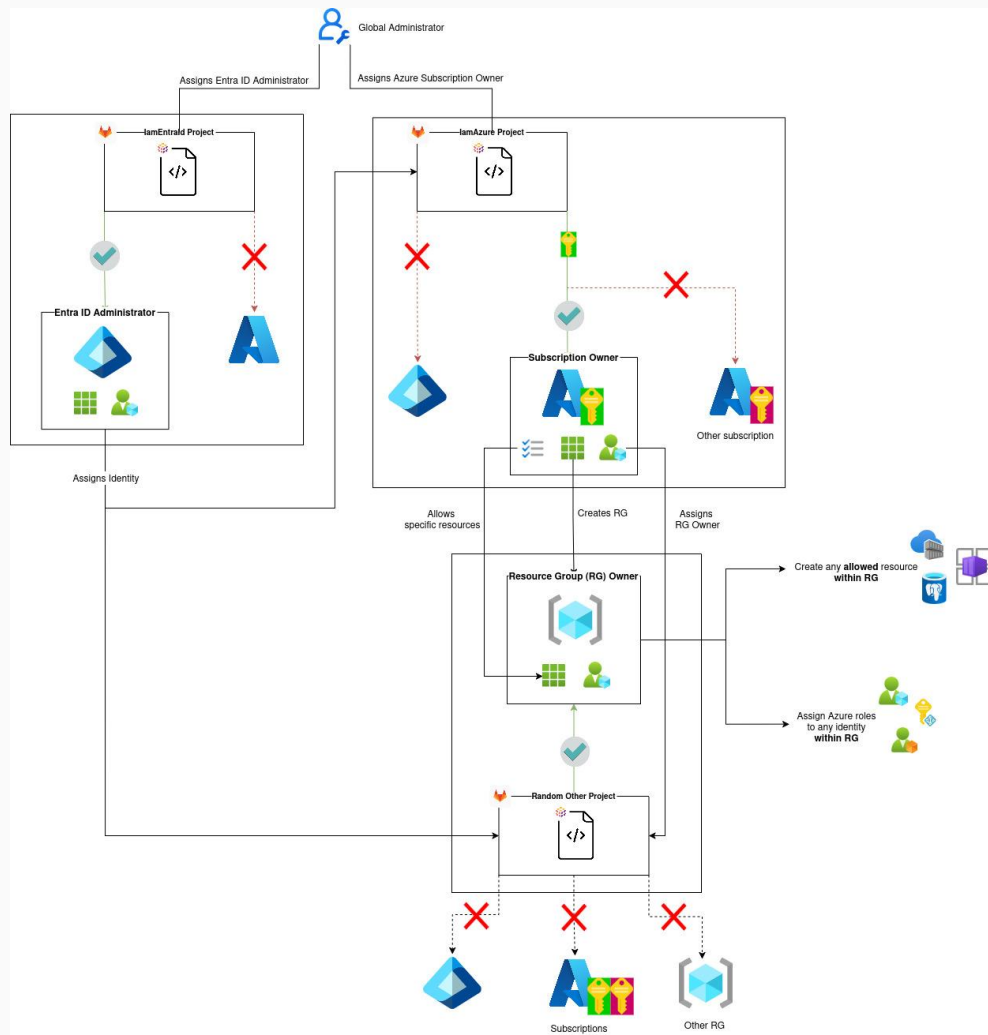
- Administrator
- Only Entra ID resources & roles

- **lamAzure workload:**

- Owner of a subscription
- Only Azure resources & roles
- Allows resource providers

- **Other workloads:**

- Owner of a Resource Group (RG)
- Only RG resources & roles
- Only allowed resource providers



Result

Result

Overview

- Successfully implemented a scalable workload IAM template suite
 - Improved security, consistency, and maintainability with **IaC** principles
 - Further improved security and maintainability with **Credential-Free** workload authentication
 - Simplified adoption with customizable **templates**
 - Enhanced feature support with **workarounds**

Result

Requirements

Functional Requirements		
ID	TITLE	STATUS
FR1	Install Template Suite	🚧
FR2	Generate Projects from Templates with Custom Parameters	🚧
FR3	Publish NuGet Packages for Common Components	✅
FR4	Setup IAM-provisioning IaC Projects	✅
FR5	Include CI/CD pipelines in projects	✅
FR6	Manage IAM-provisioning IaC Projects	✅
FR7	Provision Microservice Resources	✅
FR8	Access Microservice Resources	✅

Non-Functional Requirements		
ID	TITLE	STATUS
QR1	Optimized System Performance	✅
QR2	Code Readability	😬
QR3	Reusable Components & Modularization	✅
QR4	Testability	✅
QR5	Documentation	✅
QR6	Credential-free Workload Identities	✅
QR7	IAM Role Least Privilege Enforcement	😬

Analysis and Discussion

Analysis and Discussion

Challenges

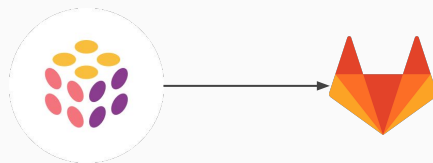
- Missing features in providers
- Bugs in providers
- Financial limitations



Analysis and Discussion

Future Improvements

- Minimize manual intervention
 - Setup GitLab from Pulumi
- Extended compatibility:
 - More flexible
 - Other providers & languages
- Logging and monitoring



Questions?



Thank you!